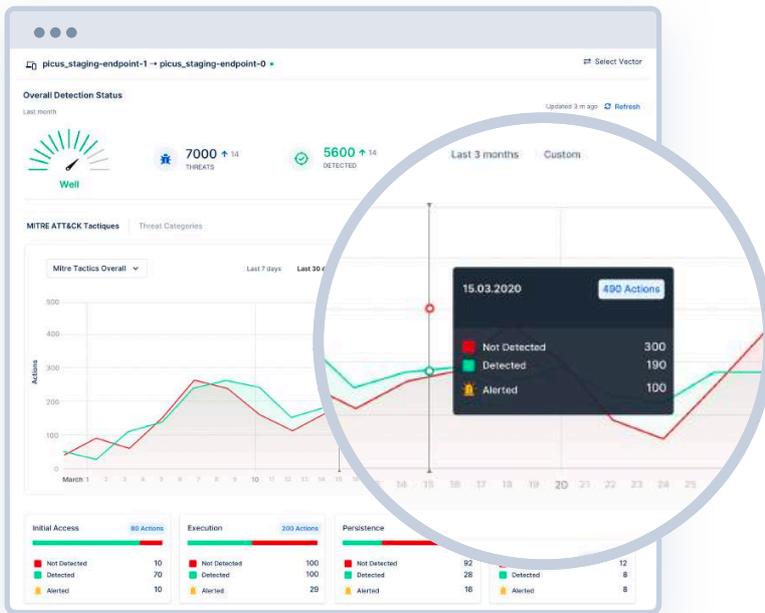


DETECTION ANALYTICS & MITIGATION

Continuous security validation that boosts detection effectiveness

Modern cyber threats require that SOC teams work hard to handle a multitude of complex data collection and analytics tasks. Processing massive volumes of information from heterogeneous environments, SOCs strive to detect all indicators of compromise swiftly, assign the right priorities and take actions without leaving anything meaningful behind. The risk is to have overly complicated security controls, inefficient budgets, and frustrated security teams. SOC teams have to make sure that logs are collected consistently, that alert fatigue resulting from inefficient SIEM rules is minimised, and that cross-team communication and reporting are streamlined.

Picus Detection Analytics & Mitigation is a threat-centric, multi-component solution based on Picus Threat Library, Detection Analytics Module and Mitigation Library that allows SOC teams to highlight risks associated with data collection challenges and exposes undetected malicious activities. The solution offers easy-to-implement mitigation suggestions and updates, improving SOC processes across the board – from threat intelligence to incident analysis and incident response.



DELIVERING FALSE-POSITIVE FREE RESULTS

Picus Detection Analytics is designed to provide minimal to zero false positives thanks to its wide angled analytics capabilities that can process large sets of data over multiple network segments and security control activities.



THREAT CENTRIC DETECTION ANALYTICS

Picus Detection Analytics has an intelligent 24x7 modus operandi. It utilizes the most extensive adversarial context, covering more than 90% of the MITRE ATT&CK techniques and the largest number of malware, vulnerability exploits, and web application attacks samples, thanks to Picus Threat Library.



GOING BEYOND "VISIBILITY ONLY" APPROACHES

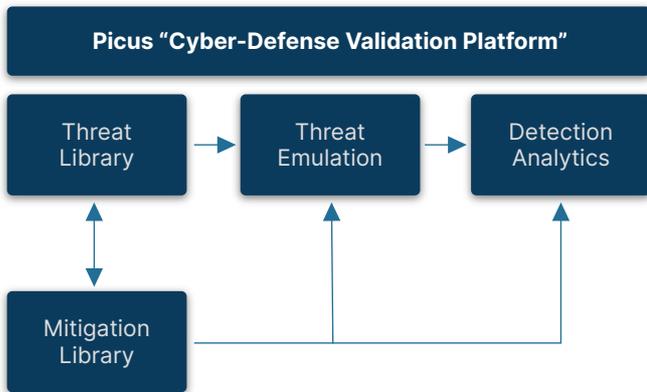
The unique integration between the Detection Analytics and Mitigation Library makes vendor-specific EDR and SIEM detection policy improvements easy and possible. Picus' existing technology alliance partners in this category are IBM, Splunk, and VMware Carbon Black.

HIGHLIGHTS

- Log Collection Validation**
 Remove your blind spots by collecting required level of logs for SOC operations and assess detection capabilities on existing vectors to gain visibility to undetected gaps.
- Improve Alerting Capability**
 Assess and improve alerting capabilities and avoid any human-related shortcomings and errors on detection content.
- Visualize Residual Risk**
 Measure, report, and communicate technical risk with stakeholders and identify configuration problems to enhance the security stack.
- Decrease Dwell Time**
 Decrease delay between attack occurrence and alert generation and increase the value delivered by the Detection products.
- Targeted Mitigation Advice**
 Our vendor-specific mitigation advice covers a large set of security controls sourced from our Technology Alliance Ecosystem for instant mitigation.

HOW IT WORKS

The Picus Detection Analytics and Mitigation solution consists of Picus Threat Library, Detection Analytics Module, and Mitigation Library. While adversarial content from the Threat Library is used to run assessments, the Detection Analytics Module continually processes log and event monitoring data matching patterns, and the Mitigation Library reveals available signatures and policies developed by the vendors to address the identified security control gaps.



PICUS MITIGATION LIBRARY

While Picus Labs' Red Team adds new adversarial content to the Threat Library, the Blue Team examines the solution inventory of Picus' technology partners to enrich each threat and technique sample with mitigation alternatives. New threats and associated mitigation alternatives are added daily.

Picus Mitigation Library provides vendor-specific policy insights for the following categories: network security controls, next-generation firewall, network intrusion prevention systems, web application firewalls, Endpoint Detection & Response (EDR) solutions, SIEM platforms.

PICUS DETECTION ANALYTICS MODULE

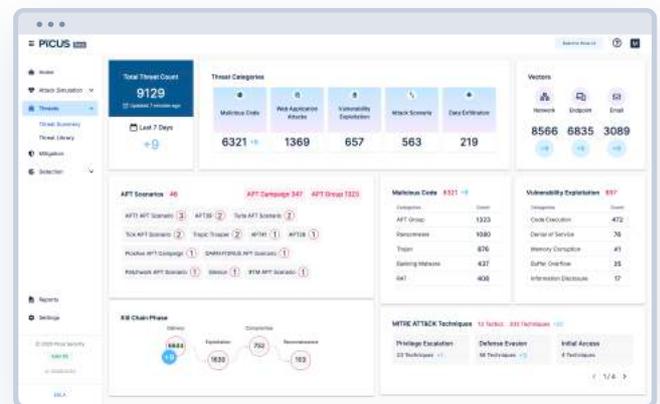
Picus Detection Analytics is an automated module that queries SIEM and EDR security logs to find the difference between the available and expected. Every emulated threat and adversary technique creates a log in the relevant security controls should these emulations be detected or prevented. Querying SIEM and EDR platforms in customer environments, the Picus Detection Analytics module matches query findings using advanced algorithms, with the real threat samples and techniques emulated by Picus Threat Emulation Module. As a result, undetected, unlogged, and non-alerted attacks are identified on the spot.

Detection Analytics Module adds intelligence to the query findings by providing alert validation, log granularity concerning deployed security control technologies and MITRE ATT&CK mapping.

PICUS THREAT LIBRARY

Picus Threat Library contains thousands of daily-updated malware, vulnerability exploits, web application attack samples, and atomic adversarial techniques selected via commonality evaluation of global threat watch data. Hundreds of nation-state and vertical driven attack scenarios are included. Content is mapped to the frameworks of MITRE ATT&CK, Cyber Kill Chain, and OWASP and presented in relation to targeted applications, targeted operating systems, severity level as well as Common Vulnerabilities and Exposures/Common Weakness Enumeration (CVE/CWE) references.

Through the Threat Library, users find samples of the most recent adversarial techniques at their fingertips, allowing them to stay ahead of newest threats, saving the hassle of setting up and maintaining an in-house repository. SOC analysts, threat hunters and incident responders, security operations teams, red team and pen-testers can utilize this granular content for various testing scenarios.



TECHNOLOGY ALLIANCES

NETWORK SECURITY



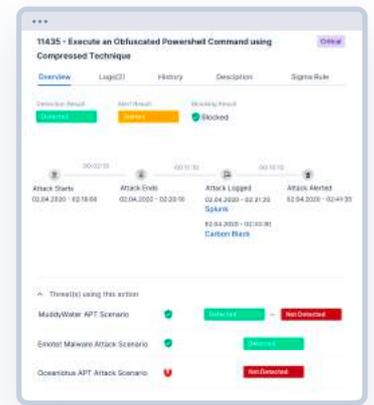
SIEM



EDR



Threats		All (7000)	Detected (3950)	Not Detected (5950)
ID	Threat Name	Severity	Latest Result Time	Log Source
764801	Minikatz Execution with Evasion by using BetterSafetyKatz	Medium	11:13:03	Net log source
304473	Win32k Denial of Service Vulnerability .EXE File Download Variant-2	Low	11:13:03	Net log source
747416	Microsoft Edge Browser RPC Marshalling Buffer Overflow Vulnerability	High	11:13:03	Net log source
712000	GulLoader Malware .EXE File Download Variant-2	High	11:13:03	Net log source
678139	Angular .JS Sandbox Escape Cross-Site Scripting	Low	11:13:03	Net log source
606810	Web Content Browsing by using InternetExplorer COM Object	High	11:13:03	Net log source
591724	Spring Cloud Config Server LFI Vulnerability Variant-2	Low	11:13:03	Net log source
581235	GulLoader Malware .BIN File Download Variant-1	High	11:13:03	Net log source
306800	GulLoader Malware .EXE File Download Variant-1	High	11:13:03	Net log source
889525	KenDown Downloader Malware used by APT32 Threat Group .DLL File	Low	11:13:03	Net log source
888595	Linksys E-series Router Remote Code Execution (RCE) Vulnerability	High	11:13:03	Net log source
684775	Microsoft Win32k Elevation of Privilege Vulnerability	Low	11:13:03	Net log source



USE CASES



FOR SOC TEAMS

- Validate if the log mechanisms work across the whole network consistently.
- Measure detection coverage in full alignment with MITRE ATT&CK.
- Reveal the detection capabilities and configuration problems of the security stack.
- Assess and enhance alerting capabilities of SIEM platforms.
- Decrease the time between detection and response.
- Make residual risk visible to all stakeholders.
- Empower threat hunters and incident responders by providing real threat samples and specific validation capacity.
- Request test scenarios from red-team practitioners relevant to detection shortcomings and get insights that will have the immediate impact on cyber-defense capabilities.
- Increase the detection capabilities of security controls by instrumenting Picus Mitigation library and achieving a threat informed communication with IT SecOps teams.



FOR SECURITY LEADERS

- Gain visibility over post-compromise detection in addition to the prevention capabilities provided by Picus Security Control Validation & Mitigation Solution.
- Increase operational efficiencies by identifying possible misalignments between people, process and technologies, concerning Information Technology and Cyber Security.



FOR SecOps MANAGERS

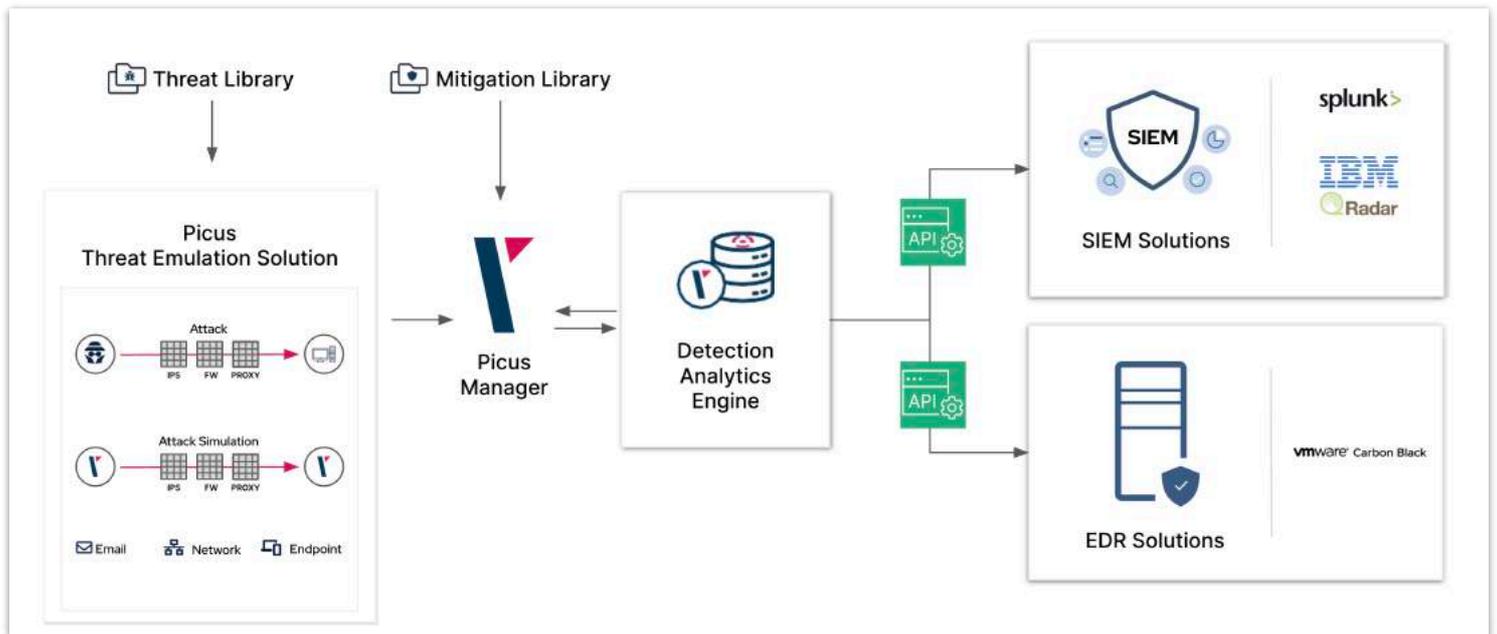
- Understand and fix infrastructure related problems that may affect cyber-security operations and efficacy.



FOR RED TEAMERS

- Prioritise test scenarios relevant to detection shortcomings and deliver insights that will have immediate impact on cyber-defense capabilities.

REQUIREMENTS



Picus Manager

VMware ESX/i 5.1 or later. Hyper-V Server 2008 and later. Physical Servers: Any hardware supporting CentOS 7 x64 (minimal installation).
4 GB memory,
50 GB disk space,
one network interface

Picus Network and Email Peer

VMware ESX/i 5.1 or later. Hyper-V Server 2008 and later. Physical Servers: Any hardware supporting CentOS 7 x64 (minimal installation).
2 GB memory,
20 GB disk space,
one network interface

Picus Endpoint Peer

Supports Windows 7 SP1, Windows 8.1, Windows 10, Windows Server 2012 R2 and Windows Server 2016 with .NET Framework 4.5.2 or above.
4 GB memory,
20 GB disk space,
one network interface

DEPLOYMENT COMPONENTS

Picus Manager – provides an easy-to-use web user interface from which Picus assessments and reports are managed.

Picus Network and Email Peer – A vector defines the network path followed by an attack. Any vector terminates in two peers (an attacker and a victim). A network peer can be selected either as a victim or attacker peer.

Picus Endpoint Peer – Simulation peer to test endpoint security. It can only be configured as a victim peer.

Picus Integration Peer – provides integration with security solutions/systems in the customer environment for Picus Security modules.

DEPLOYMENT OPTIONS

Picus Manager - Available as HyperV and VMware virtual images or also available on physical/virtual servers which support CentOS 7 x64.

Picus Network and Email Peer – Available as HyperV and VMware virtual images. It is also possible to install Picus Peers to physical servers and PCs which support CentOS 7 x64.

Picus Endpoint Peer – Runs on Microsoft Windows. Picus does not distribute any Endpoint Peer image. It is expected that Endpoint Peer is to be installed on an instance of the organization's Windows golden image.

Picus Integration Peer – Available as HyperV and VMware virtual images. It is also possible to install Picus Peers to physical servers and PCs which support CentOS 7 x64.

PICUS

About Picus

Picus Security is a breach and attack simulation (BAS) vendor. BAS was categorized as a new security assessment domain in 2018 by Gartner, and Picus has been named as a Cool Vendor in 2019. Picus is an intelligence-driven security validation platform that simplifies security operations and optimizes defenses. The platform safely emulates cyber threats and provides mitigation guidance - allowing organizations to improve visibility and security investment utilization.